Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The FTC Has Already Set Cybersecurity Standards

Law360, New York (March 05, 2015, 2:07 PM ET) --

Bruce Heiman

In January, the president and congressional leaders called for cooperation in passing cybersecurity legislation to address the growing threats faced by American businesses and consumers. The president called for Congress to pass legislation that would establish a federal data breach standard and give the Federal Trade Commission enforcement and rulemaking authority to implement the law. Legislation has already been introduced in the Senate and House directing the FTC to promulgate regulations requiring entities that own or possess personal information to have policies and procedures to protect that information.[1]

While such legislation and subsequent regulations would clarify a generally applicable federal cybersecurity standard, in fact the FTC has already set such standards. No, you can't find them in a statute or the Code of Federal Regulations. And, as the proposed legislation implicitly recognizes, the FTC currently does not have specific authority to promulgate cybersecurity regulations (even if it might have general authority to issue rules under the Federal Trade Commission Act). Instead, the FTC has de facto established the standards by bringing dozens of enforcement actions under its general statutory authority — Section 5(a) of the Federal Trade Commission Act — to address "unfair or deceptive acts or practices in or affecting commerce."[2]

The FTC began addressing cybersecurity in 2000 by taking action against companies that claimed that they took various measures to protect information but, in practice, failed to do so. The FTC alleged in six cases from 2000 to 2005 that the company had engaged in deceptive acts, essentially by misrepresenting to consumers the nature of the company's cybersecurity/privacy protections. Each time, the FTC and the company agreed to settle the action under consent decrees running as long as 20 years. The company agreed not to claim it was doing more than it actually did and to adopt a cybersecurity program that was designed to establish and maintain reasonable and appropriate administrative, technical, and physical safeguards.

However, beginning in 2005 with the BJ's Wholesale Club case,[3] the FTC began to bring actions against companies whose cybersecurity practices it deemed to be inherently "unfair" or unreasonable, independent of whether the company had made any claims about its security practices. In eight cases since the BJ's Wholesale Club case, the FTC has relied exclusively upon its "unfairness" authority to

establish de facto cybersecurity standards for a broad swath of the American economy (without also asserting a deception claim).[4] These nine cases therefore appear to establish the minimum required by the FTC with respect to "reasonable" cybersecurity practices. The agency has required other measures of particular companies when they also claimed to protect particular information and failed to do so (hence, the FTC found them to be "deceptive" acts). It remains unclear whether the FTC would find the absence of such measures to be inherently unfair and unreasonable absent the claims.

During the past 15 years, the FTC has also instituted numerous enforcement actions involving alleged violations of other specific laws within the FTC's cybersecurity enforcement jurisdiction, including the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act and the Children's Online Privacy Protection Act, among others. These statutes govern the information security of specific industries (e.g., the Gramm-Leach-Bliley Act applies to financial institutions) or specific types of information (e.g., the Fair Credit Reporting Act applies to information contained in credit reports). At times, the FTC has asserted that violations involving these particular laws either triggered or coexisted alongside violations of the FTC Act (both unfairness and deception). It is unclear whether the FTC would have found certain conduct to be "unfair" or "deceptive" had the company not otherwise violated one of these additional, specific statutes.

Below, we summarize those measures that the FTC apparently expects companies to adopt as part of a reasonable data security program, in light of the FTC's 15-year enforcement history in this space. We focus on those nine cases that exclusively target "unfairness," as these cases apparently include those baseline measures that the FTC believes should be adopted to satisfy reasonable administrative, technical and physical controls — the standard that companies must meet, according to the FTC.

Administrative Measures

Information Security Program

As a starting point, companies must develop and disseminate information security programs that are designed to: (1) designate one or more employees to coordinate the program; (2) identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assess the sufficiency of any safeguards in place to control those risks; (3) design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures; (4) oversee service providers and require them by contract to protect the security and confidentiality of customer information; and (5) evaluate and adjust the program in light of the results of testing, monitoring, changes to the business operation, and the other relevant circumstances.[5] This process would necessarily require a company to memorialize its information security policies and procedures in writing.

Incident Response Plan

One component of any reasonable cybersecurity plan is what to do in the event that there is an unauthorized release of confidential or protected personal information.[6]

Training

It is not enough to simply publish a security plan — companies must also implement sufficient training programs for their employees to help ensure the safeguarding of sensitive information.[7]

Storing Data

While the company can and should deploy technical measures to protect information (see below), the more fundamental question is whether the company is keeping information that it no longer needs. The FTC has criticized companies for retaining information for longer than needed,[8] in multiple redundant files,[9] and on portable devices[10] — all when the information was not needed for business purposes.

No Unauthorized Applications

The FTC has found that the failure not only to prohibit unauthorized applications on a company's network, but also to scan the network to detect whether there is any unauthorized software (e.g., peer-to-peer file-sharing) is unreasonable.[11]

Responding to Security Warnings

The FTC has criticized companies for failing to follow up on security warnings and intrusion alerts to help prevent future breaches.[12]

Monitoring and Logging of Activity

While this is a technical function (see below), the company's information security policy should require that activity on a company's network be monitored and logged to detect unusual activity, unauthorized access, or unexplained traffic (i.e., inbound and outbound transfers of information).[13]

Technical Measures

Failure to Use Simple, Low-Cost, Available Defenses

In several cases, the FTC has charged companies with failing to take measures that are widely recognized and not burdensome, such as staying up to date regarding software updates and patches, using appropriate firewalls and strong passwords, or employing measures to ensure that information sent to employees' personal email accounts is not subject to unauthorized disclosure.[14]

Credentials

The FTC has brought a number of cases involving companies' failure to take measures to sufficiently authenticate those who seek to use a company's computer system or Web interface. It has been as simple as not using a default, out-of-the-box, user identifications and passwords, or allowing persons to create new login credentials without confirming their identity.[15] But the FTC has gone further, requiring strong passwords (not common dictionary words, or the same password and username); periodic changes to user credentials (e.g., every 90 days); two-factor authentication controls; and different passwords for different access programs.[16] The FTC also requires that credentials not be shared or stored in a vulnerable format and that they be suspended after a certain number of unsuccessful log-in attempts.[17]

Access

In several cases in the retail environment the FTC has focused on the failure to secure access to a

network through wireless connections.[18] The FTC similarly has cited retailers that have not prevented access from one in-store computer to others on the network or to the Internet. Companies should, therefore, employ firewalls to segregate networks.[19] The FTC's concern also extends to a company's failure to secure third parties connecting to its computer network.[20] This includes the failure to restrict access to a network by restricting connections to specific IP addresses.[21] The FTC has also criticized companies that grant employees access to personal information that is not needed to perform the employees' jobs.[22]

Encryption

The failure to encrypt information kept in storage or during transmission has been deemed an unreasonable practice.[23] This issue crops up for information transmitted through/stored on company websites and servers, as well as information stored on employees' computers. Companies have found themselves in the crosshairs of FTC enforcement when employees' laptops that contain unencrypted, personal information are stolen.[24]

Software

The agency expects companies to patch and update cybersecurity software such as antivirus software.[25]

Monitoring

Continuous monitoring and logging of activity facilitate a comprehensive view to what is happening on the firm's network. Intrusion-detection procedures help identify actual and attempted attacks and malicious software.[26]

Physical

Data Disposal

Although the FTC has not addressed physical data disposal in the nine cases that we cite above, we note that there have been a number of cases in which companies simply dumped hard-copy printouts of various materials containing sensitive personal information into a waste receptacle rather than burning, pulverizing or shredding it.[27] The FTC has deemed this to be an unreasonable practice.

Conclusion

Although the FTC has not issued specific guidance delineating the universe of cybersecurity practices that it deems to be unreasonable (assuming, arguendo, it has the authority to do so), the agency has essentially done just this through a 15-year trail of enforcement actions. Until such time as the FTC promulgates rules delineating specific cybersecurity standards, companies must continue to read the tea leaves of FTC enforcement actions (alongside industry best practices) to glean the ever-changing requirements of "reasonable" cybersecurity practices.

—By Bruce J. Heiman, Soyong Cho and Andrew L. Caplan, K&L Gates LLP

Bruce Heiman is a partner in K&L Gates' Washington, D.C., office and co-chairs the policy and regulatory practice. Soyong Cho is a partner and Andrew Caplan is an associate in the firm's Washington office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See Data Security and Breach Notification Act of 2015, S. 117, 114th Cong. (2015); see also Personal Data Privacy and Security Act of 2014, H.R. 3990, 113th Cong. (2014).

[2] This authority has been recently challenged by defendants in two separate cases: FTC v. Wyndham and In re the Matter of LabMD Inc. To date, the United States District Court for the District of New Jersey in the Wyndham case has been the only federal court to reach the merits of the FTC's cybersecurity authority. The District of New Jersey upheld this authority; an appeal is pending before the Third Circuit Court of Appeals. See FTC v. Wyndham Worldwide Corporation, et al., No. 2:13-cv-01887-ES-JAD (D.N.J.) (April 7, 2014).

[3] See In the Matter of BJ's Wholesale Club Inc., FTC No. 042-3160 (Sep. 20, 2005) (complaint).

[4] See In the Matter of DSW Inc., FTC No. 052-3096 (Mar. 7, 2006) (complaint); In the Matter of CardSystems Solutions Inc., FTC No. 052-3148 (Sep. 5, 2006) (complaint); In the Matter of the TJX Companies Inc., FTC No. 072-3055 (Jul. 29, 2008) (complaint); In the Matter of Reed Elsevier Inc. and Seisint Inc., FTC No. 0523094 (Jul. 29, 2008) (complaint); In the Matter of Dave & Buster's Inc., FTC No. 082-3153 (May 20, 2010) (complaint); In the Matter of EPN Inc., FTC No. 112-3143 (Oct. 3, 2012) (complaint); In the Matter of LabMD Inc., FTC No. 102-3099 (Aug. 28, 2013) (complaint); In the Matter of Accretive Health Inc., FTC No. 122-3077 (Feb. 5, 2014) (complaint).

[5] See e.g., In the Matter of EPN Inc., FTC No. 112-3143 (Oct. 3, 2012) (decision and order).

[6] See e.g., In the Matter of EPN Inc. (complaint).

[7] See id. Note that in a case involving alleged unfairness and deception, the FTC asserted that employee training should extend to engineering staff. See In the Matter of HTC America Inc., FTC No. 122-3049 (June 25, 2013) (complaint).

[8] See e.g., In the Matter of BJ's Wholesale Club Inc. (complaint).

[9] See e.g., In the Matter of DSW Inc. (complaint).

[10] See e.g., In the Matter of Accretive Health Inc. (complaint).

[11] See e.g., In the Matter of EPN Inc. (complaint).

[12] See e.g., In the Matter of The TJX Companies Inc. (complaint). In cases in which the FTC has alleged that companies engaged in both unfair and deceptive acts and practices, the FTC has criticized companies for failing to have a process to receive and address vulnerability reports. See e.g., In the Matter of HTC America Inc. (complaint).

[13] See e.g., In the Matter of Dave & Buster's Inc. (complaint).

[14] See e.g., In the Matter of CardSystems Solutions Inc., (complaint).

[15] See e.g., In the Matter of BJ's Wholesale Club Inc.(complaint); see also In the Matter of Reed Elsevier Inc. and Seisint Inc. (complaint).

[16] See e.g., In the Matter of CardSystems Solutions Inc., (complaint); see also In the Matter of The TJX Companies Inc. (complaint); see also In the Matter of Reed Elsevier Inc. and Seisint Inc. (complaint); see also In the Matter of LabMD Inc. (complaint).

[17] See e.g., In the Matter of Reed Elsevier Inc. and Seisint Inc. (complaint).

[18] See e.g., In the Matter of BJ's Wholesale Club Inc. (complaint).

[19] See e.g., In the Matter of DSW Inc. (complaint); see also In the Matter of Dave & Buster's Inc. (complaint).

[20] See e.g., In the Matter of BJ's Wholesale Club Inc. (complaint).

[21] See e.g., In the Matter of Dave & Busters Inc. (complaint).

[22] See e.g., In the Matter of Accretive Health Inc. (complaint).

[23] See e.g., In the Matter of The TJX Companies Inc. (complaint).

[24] See e.g., In the Matter of Accretive Health Inc., (complaint). In a case involving both alleged unfairness and deception, the FTC criticized a company for storing login credentials in plain text. See In the Matter of TRENDnet Inc., FTC No. 122-3090 (Jan. 16, 2014) (complaint). In another case involving alleged deception, the FTC also criticized a company for including unencrypted information on backup tapes. See In the Matter of CBR Systems Inc., FTC No. 122-3120 (Apr. 29, 2013).

[25] See e.g., In the Matter of The TJX Companies Inc. (complaint). In at least two matters in which the FTC alleged both unfairness and deception, the agency has criticized companies for failing to review and test software that they develop (albeit through third-party contractors) for cybersecurity vulnerabilities. See e.g., In the Matter of HTC America Inc. (complaint); see also In the Matter of TRENDnet Inc. (complaint).

[26] See e.g., In the Matter of BJ's Wholesale Club Inc. (complaint); see also In the Matter of DSW Inc. (complaint).

[27] See e.g., In the Matter of CVS Caremark Corporation, FTC No. 072-3119 (June 18, 2009) (complaint).
